

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.2
TẤN CÔNG VÀO MẬT KHẨU**

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

| | |
|---|----------|
| MỤC LỤC..... | 2 |
| CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH..... | 3 |
| 1.1 Mục đích..... | 3 |
| 1.2 Lý thuyết bài thực hành..... | 3 |
| 1.2.1 Phương pháp bẻ khóa mật khẩu | 3 |
| 1.2.2 Công cụ Crack mật khẩu | 3 |
| CHƯƠNG 2. nội dung thực hành..... | 6 |
| 2.1 Chuẩn bị môi trường | 6 |
| 2.1.1 Cài đặt phần mềm ảo hóa | 6 |
| 2.1.2 Cài đặt hệ điều hành | 6 |
| 2.1.3 Cài đặt công cụ Crack mật khẩu trên Linux | 6 |
| 2.1.4 Cài đặt công cụ Crack mật khẩu trên Windows | 6 |
| 2.2 Các bước tiến hành..... | 7 |
| 2.2.1 Trên hệ điều hành Linux | 7 |
| 2.2.2 Trên hệ điều hành Windows..... | 9 |
| KẾT LUẬN | 13 |
| TÀI LIỆU THAM KHẢO..... | 13 |

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

- Hiểu được mối đe dọa về tấn công mật khẩu.
- Hiểu được nguyên tắc hoạt động của một số công cụ Crack mật khẩu trên các hệ điều hành Linux và Windows.
- Biết cách sử dụng công cụ để Crack mật khẩu trên các hệ điều hành Linux và Windows.

1.2 Lý thuyết bài thực hành

1.2.1 Phương pháp bẻ khóa mật khẩu

Trước khi đến công đoạn bẻ khóa mật khẩu, bạn phải biết về ba nhân tố xác thực:

- Thứ tôi có, ví dụ như tên user và mật khẩu.
- Thứ tôi là, ví dụ như sinh trắc học (dấu vân tay).
- Thứ tôi sở hữu, ví dụ như thiết bị đã đăng ký/ được cấp phép

Bẻ khóa mật khẩu là quá trình trích rút mật khẩu để nhận quyền truy cập vào mục tiêu như một user chính thống. Thông thường, chỉ có quyền xác minh mật khẩu hay tên tài khoản được thiết lập. Tuy nhiên hiện nay, quyền xác minh mật khẩu được tạo thành từ nhiều nhân tố, bao gồm những thứ bạn có như tên tài khoản, mật khẩu và sinh trắc học.

Do đó, có thể sử dụng tấn công phi kỹ thuật hoặc quấy nhiễu đường truyền tin để bẻ khóa mật khẩu. Mật khẩu ngắn, dễ đoán, độ mã hóa thấp hay chỉ gồm số và chữ là những loại mật khẩu có thể bẻ khóa dễ dàng. Một mật khẩu dài và khó đoán sẽ là biện pháp phòng thủ đầu tiên trước những tấn công như thế này. Một mật khẩu tốt tiêu biểu sẽ chứa:

- Các kiểu chữ khác nhau (chữ hoa, chữ thường)
- Ký tự đặc biệt
- Số
- Độ dài (thường nhiều hơn 8 ký tự)

1.2.2 Công cụ Crack mật khẩu

1.2.2.1 John the Ripper

John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu ban đầu được phát triển cho hệ điều hành Unix. Nó là một trong những chương trình testing/breaking mật khẩu phổ biến nhất vì có kết hợp một số bộ cracker mật khẩu trong cùng một gói phần mềm, tự động phát hiện các kiểu mật khẩu và có một bộ cracker có khả năng tùy chỉnh. Công cụ này có thể được chạy cho các định dạng mật khẩu đã được mã hóa chẳng hạn như các kiểu mật khẩu mã hóa vẫn thấy trong một số bản Unix khác (dựa trên DES, MDS hoặc Blowfish), Kerberos AFS và Windows NT/2000/XP/2003 LM hash. Bên cạnh đó còn có các module bổ sung mở rộng khả năng gồm có cả các kiểu mật khẩu MD4 và các mật khẩu được lưu trong LDAP, MySQL và các thành phần khác.



```
Finished - John

John the Ripper Version 1.0 ALPHA 2 Copyright (c) 1996 by Solar Designer

Usage: [john [flags] [passwd file]]

Flags: -pwfile:<file>[,...] specify passwd file(s) (wildcards allowed)
       -wordfile:<file> -stdin wordlist mode, read words from <file> or stdin
       -rules enable rules for wordlist mode
       -incremental[:<mode>] incremental mode [using john.ini entry <mode>]
       -single single crack mode
       -external:<mode> external mode, using john.ini entry <mode>
       -restore[:<file>] restore session [from <file>]
       -makechars:<file> make a charset, <file> will be overwritten
       -show show cracked passwords
       -test perform a benchmark
       -users:<login|uid>[,...] crack this (these) user(s) only
       -shells:[!]<shell>[,...] crack users with this (these) shell(s) only
       -salts:[!]<count> crack salts with at least <count> accounts only
       -lamesalts assume cleartext passwords were used as salts
       -timeout:<time> abort session after a period of <time> minutes
       -list list each word
       -keep quiet keep or don't keep when a password is found
       -nomame -nohash don't use memory for login names or hash tables
```

1.2.2.2 Hash Suite

Hash Suite, giống như tất cả các trình bẻ khóa băm mật khẩu khác, không cố gắng "đảo ngược" hàm băm để lấy mật khẩu (điều này có thể là không thể). Nó tuân theo cùng một quy trình được sử dụng trong xác thực: nó tạo ra các mật khẩu ứng viên khác nhau (khóa), băm chúng và so sánh các hàm băm đã tính toán với các hàm băm đã lưu trữ.

Phương pháp này hiệu quả vì người dùng thường chọn mật khẩu dễ nhớ và như một tác dụng phụ, những mật khẩu này thường dễ bị bẻ khóa. Một lý do khác khiến cách tiếp cận này rất hiệu quả là Windows sử dụng các hàm băm mật khẩu có tốc độ tính toán rất nhanh, đặc biệt là trong một cuộc tấn công (cho mỗi mật khẩu ứng viên được đưa ra).

Hash Suite cung cấp một số cách khác nhau (được gọi là key-providers) để tạo mật khẩu ứng viên (đôi khi được gọi là khóa):

- Charset: Tạo khóa bằng cách thử tất cả các kết hợp của một charset nhất định. Còn được gọi là brute-force.
- Wordlist: Tạo khóa bằng cách lấy chúng từ một từ điển. Rất thành công và cần ít tài nguyên.
- Keyboard: Tạo khóa bằng cách thử kết hợp các phím liên kề trên bàn phím.
- Phrases: Tạo cụm từ kết hợp các từ từ danh sách từ. Hữu ích để thử mật khẩu dài.
- DB Info: Tạo khóa bằng cách lấy tất cả tên người dùng/mật khẩu tìm thấy. Hữu ích khi bất quy tắc.
- LM2NT: Thay đổi chữ hoa chữ thường của các ký tự trong mật khẩu băm LM đã bẻ khóa để bẻ khóa ngay lập tức mật khẩu băm NTLM tương ứng.

Hash Suite cũng hỗ trợ các quy tắc có thể áp dụng cho tất cả các key-providers. Quy tắc là những chuyển đổi phổ biến sang các từ cơ bản mà nhiều người dùng thực hiện để tạo thành mật khẩu (ví dụ, từ "love" có thể tạo ra mật khẩu là "Love12").

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

2.1.1 Cài đặt phần mềm ảo hóa

- VMWare Workstation

2.1.2 Cài đặt hệ điều hành

- Một máy ảo Linux (Kali Linux)
- Một máy ảo Windows

2.1.3 Cài đặt công cụ Crack mật khẩu trên Linux

- Dùng công cụ John the Ripper: `sudo apt install john`
- Kiểm tra phiên bản John bằng lệnh: `john | head -n 1`

```
(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ john | head -n 1
Created directory: /home/b22dcat253/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100
OMP [linux-gnu 64-bit x86_64 AVX2 AC]

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ date
Sat Apr 5 01:37:08 AM EDT 2025

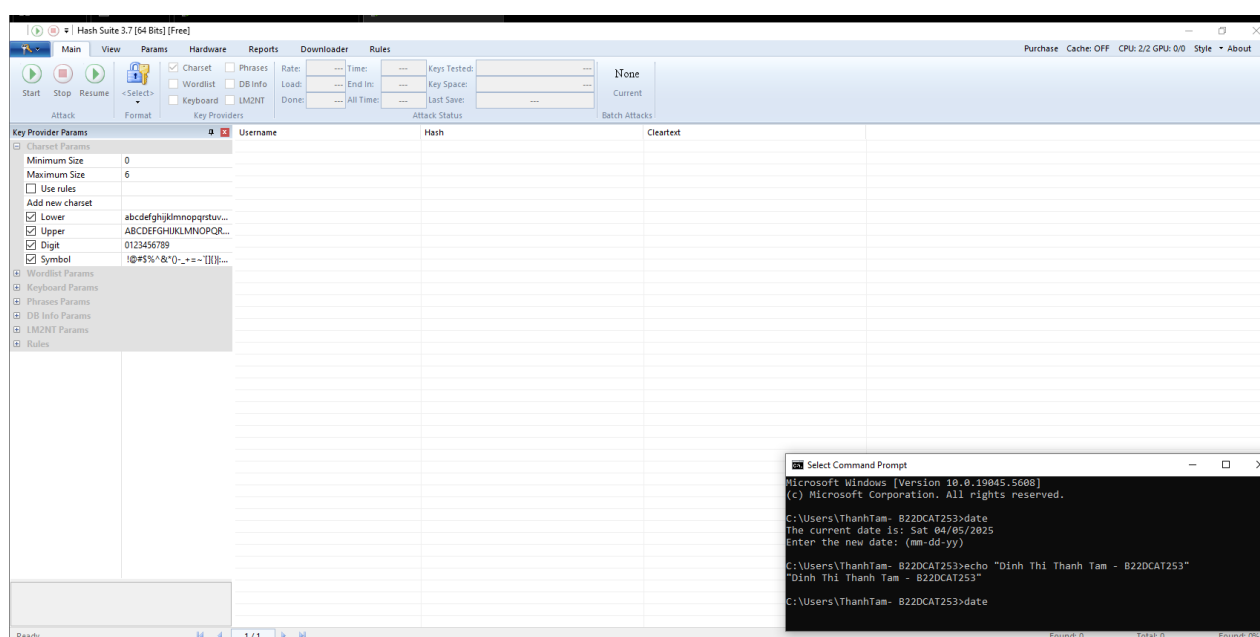
(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253
```

2.1.4 Cài đặt công cụ Crack mật khẩu trên Windows

- Dùng công cụ Hash Suite
- Tải công cụ Hash Suite để crack mật khẩu từ đường link:

<https://hashsuite.openwall.net/download>

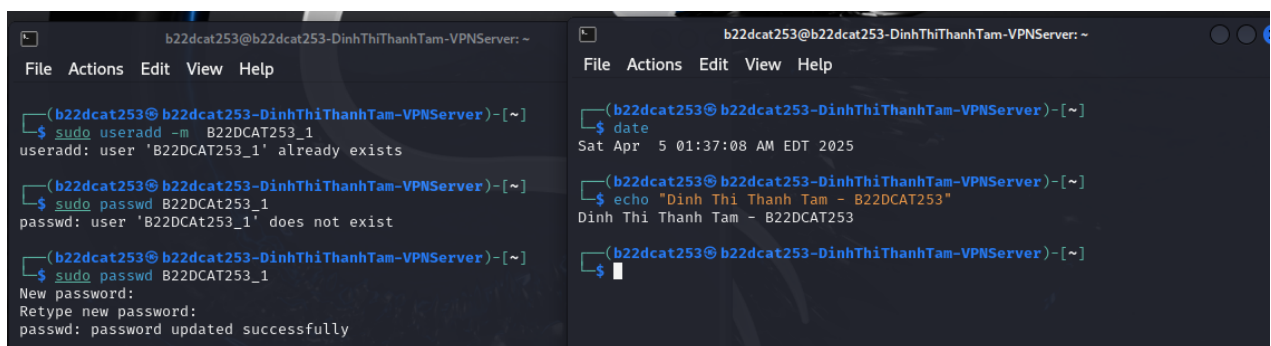


2.2 Các bước tiến hành

2.2.1 Trên hệ điều hành Linux

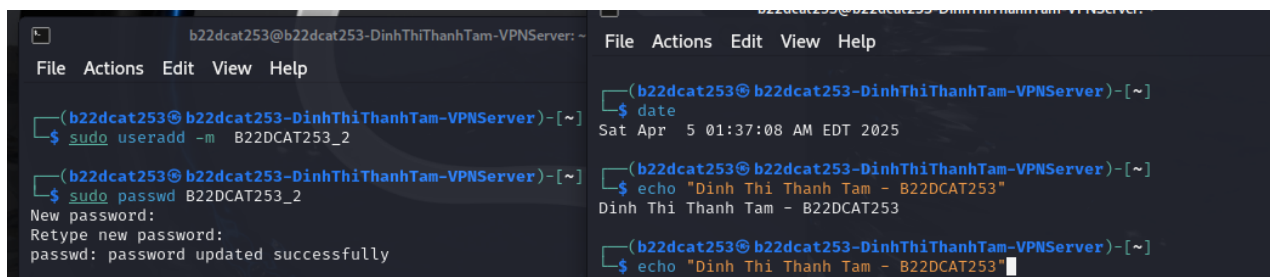
Bước 1: Tạo 3 tài khoản người dùng bắt đầu bằng mã sinh viên với mật khẩu:

- Mật khẩu 4 kí tự: B22DCAT253_1 (mật khẩu: 1234)
 - Mật khẩu 6 kí tự: B22DCAT253_2 (mật khẩu: 123456)
 - Mật khẩu 8 kí tự: B22DCAT253_3 (mật khẩu: 12345678)
- Dùng lệnh: `sudo useradd -m "username"` để tạo tài khoản mới
 - Dùng lệnh: `sudo passwd "username"` để tạo mật khẩu cho tài khoản "username"
 - Tạo tài khoản B22DCAT253_1



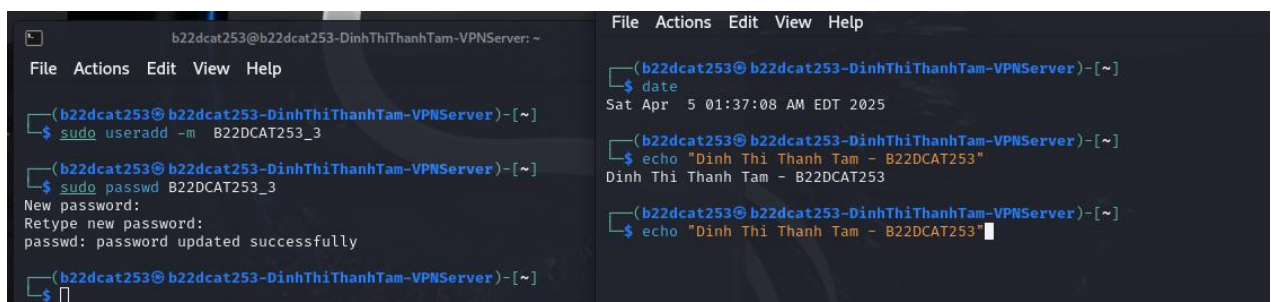
The screenshot shows two terminal windows. The left window shows the execution of `sudo useradd -m B22DCAT253_1`, which succeeds with the message "useradd: user 'B22DCAT253_1' already exists". Then, `sudo passwd B22DCAT253_1` is run, prompting for a new password (1234) and confirming it, resulting in "passwd: password updated successfully". The right window shows the date and an echo command: `echo "Đinh Thị Thanh Tam - B22DCAT253"`.

- Tạo tài khoản B22DCAT253_2



The screenshot shows two terminal windows. The left window shows the execution of `sudo useradd -m B22DCAT253_2`, which succeeds. Then, `sudo passwd B22DCAT253_2` is run, prompting for a new password (123456) and confirming it, resulting in "passwd: password updated successfully". The right window shows the date and an echo command: `echo "Đinh Thị Thanh Tam - B22DCAT253"`.

- Tạo tài khoản B22DCAT253_3



The screenshot shows two terminal windows. The left window shows the execution of `sudo useradd -m B22DCAT253_3`, which succeeds. Then, `sudo passwd B22DCAT253_3` is run, prompting for a new password (12345678) and confirming it, resulting in "passwd: password updated successfully". The right window shows the date and an echo command: `echo "Đinh Thị Thanh Tam - B22DCAT253"`.

Bước 2: Kiểm tra user đã tạo

- Dùng lệnh grep để xem thông tin tài khoản đã tạo

```
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~  
File Actions Edit View Help  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ cat /etc/passwd | grep B22DCAT253_1  
B22DCAT253_1:x:1001:1001::/home/B22DCAT253_1:/bin/sh  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ cat /etc/passwd | grep B22DCAT253_2  
B22DCAT253_2:x:1002:1002::/home/B22DCAT253_2:/bin/sh  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ cat /etc/passwd | grep B22DCAT253_3  
B22DCAT253_3:x:1003:1003::/home/B22DCAT253_3:/bin/sh  
  
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~  
File Actions Edit View Help  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ date  
Sat Apr 5 01:37:08 AM EDT 2025  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ echo "Dinh Thi Thanh Tam - B22DCAT253"  
Dinh Thi Thanh Tam - B22DCAT253  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ echo "Dinh Thi Thanh Tam - B22DCAT253"  
Dinh Thi Thanh Tam - B22DCAT253
```

Bước 3: Tạo file chứa hash mật khẩu

- Thông tin tài khoản người dùng được lưu trong file shadow. Sao chép dữ liệu vào file B22DCAT253.txt

sudo unshadow /etc/passwd /etc/shadow > B22DCAT253.txt

```
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~  
File Actions Edit View Help  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ sudo unshadow /etc/passwd /etc/shadow > B22DCAT253.txt  
[sudo] password for b22dcat253:  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$  
  
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~  
File Actions Edit View Help  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ date  
Sun Apr 6 12:19:05 PM EDT 2025  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ echo "Dinh Thi Thanh Tam - B22DCAT253"  
Dinh Thi Thanh Tam - B22DCAT253  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$
```

- File B22DCAT253.txt giờ sẽ chứa các hash mật khẩu có thể dùng cho john.
- Kiểm tra file bằng lệnh: *cat B22DCAT253.txt*, file chứa thông tin tài khoản của 3 user mới tạo

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ cat B22DCAT253.txt  
B22DCAT253_1:$y$j9T$WPAFX7oiA7PPpjGnQqa.$jeJLE.RMAN3mfWqI6KYxCXSLGTvqfWjYrq  
7FF2NEb22:1001:1001::/home/B22DCAT253_1:/bin/sh  
B22DCAT253_2:$y$j9T$R45.Bfku9r1lC0.erPdjJ.$pjGsucsmAD085rXL46Z1oJ/LN3rv4HldaC  
vhVAg0/8.:1002:1002::/home/B22DCAT253_2:/bin/sh  
B22DCAT253_3:$y$j9T$jCsSP99oIvL0myrRiUewH1$zGm8/BT/Lyk2C/k8QYArY5IwLW7iJUraF  
suQ0I/nz0:1003:1003::/home/B22DCAT253_3:/bin/sh  
  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ date  
Sun Apr 6 12:19:05 PM EDT 2025  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ echo "Dinh Thi Thanh Tam - B22DCAT253"  
Dinh Thi Thanh Tam - B22DCAT253
```

Bước 4: Crack mật khẩu bằng john

- Khởi động john để phá mật khẩu
- Trên terminal, dùng lệnh *john --format=crypt B22DCAT253.txt* và kiên nhẫn chờ đợi quá trình crack diễn ra

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ john --format=crypt B22DCAT253.txt  
Using default input encoding: UTF-8  
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/6  
4])  
Remaining 2 password hashes with 2 different salts  
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh  
a512crypt]) is 0 for all loaded hashes  
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes  
Will run 8 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
[~]  
  
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~  
File Actions Edit View Help  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ date  
Sun Apr 6 12:19:05 PM EDT 2025  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$ echo "Dinh Thi Thanh Tam - B22DCAT253"  
Dinh Thi Thanh Tam - B22DCAT253  
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]  
$
```


- Kohn đang chạy ở chế độ rules:Single và hiển thị thông báo:
Press 'q' or Ctrl-C to abort, almost any other key for status
- Ý nghĩa:
 - john đang chạy, thử crack mật khẩu từ file B22DCAT253.txt.
 - Bạn không cần chọn gì nếu muốn chương trình tự chạy đến khi hoàn tất.
 - Bạn có thể:
 - Nhấn q nếu muốn dừng lại (quit)
 - Nhấn phím bất kỳ (trừ q) để xem trạng thái hiện tại (ví dụ: % đã hoàn thành, thử bao nhiêu mật khẩu rồi,...)

Bước 5: Kết quả quá trình Crack mật khẩu diễn ra thành công hiển thị mật khẩu của các user

```

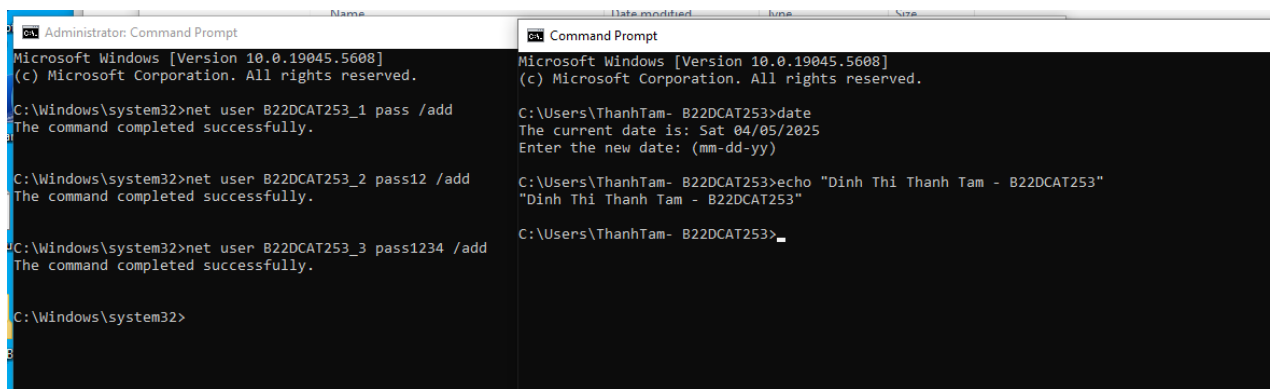
$ john --format=crypt B22DCAT253.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Remaining 3 password hashes with 3 different salts
Cost 1 (algorithm [1:decrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234 (B22DCAT253_1)
12345678 (B22DCAT253_3)
123456 (B22DCAT253_2)
3g 0:00:02:15 DONE 2/3 (2025-04-06 12:08) 0.02216g/s 191.8p/s 194.1c/s 194.1C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
  
```

2.2.2 Trên hệ điều hành Windows

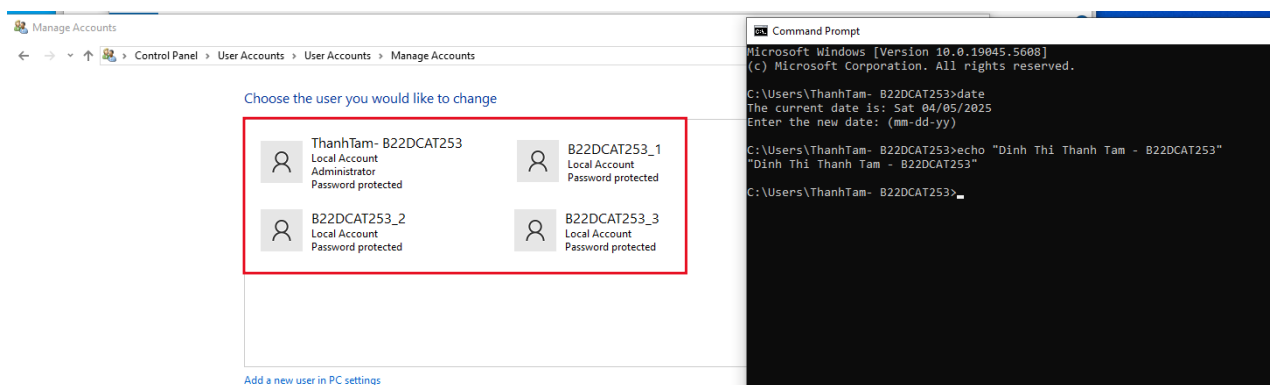
Bước 1: Tạo 3 tài khoản người dùng bắt đầu bằng mã sinh viên với mật khẩu:

- Tương tự trên Linux tạo 3 tài khoản người dùng:
 - Mật khẩu 4 kí tự: B22DCAT253_1 (mật khẩu: pass)
 - Mật khẩu 6 kí tự: B22DCAT253_2 (mật khẩu: pass12)
 - Mật khẩu 8 kí tự: B22DCAT253_3 (mật khẩu: pass1234)

Dùng lệnh: `net user "username" "password"` để tạo tài khoản "username" mới với mật khẩu "password"

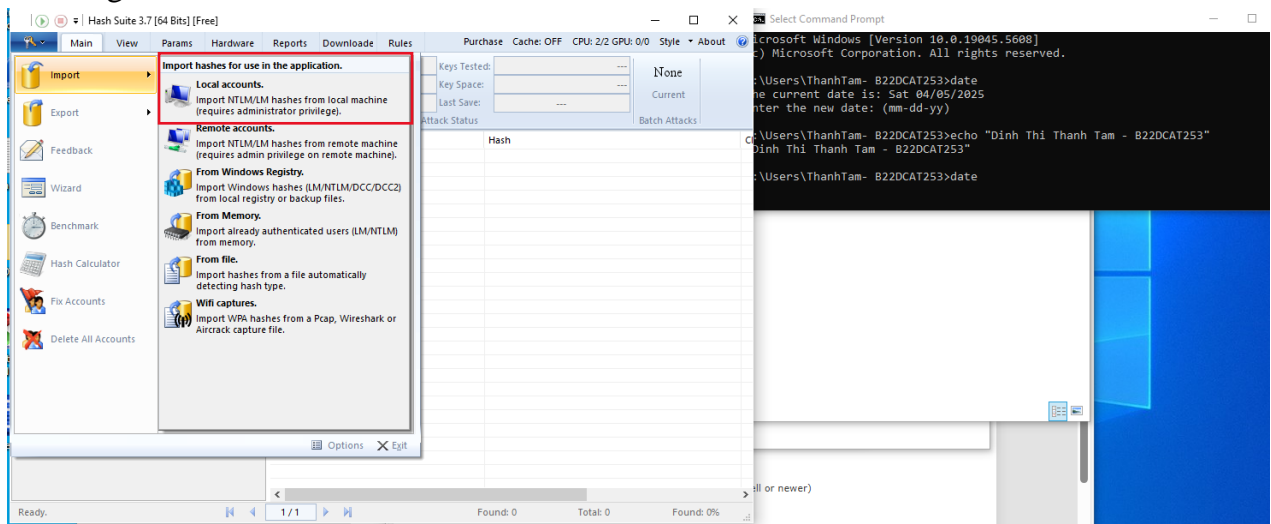


- Kiểm tra xem user đã được tạo chưa trong Manage Accounts

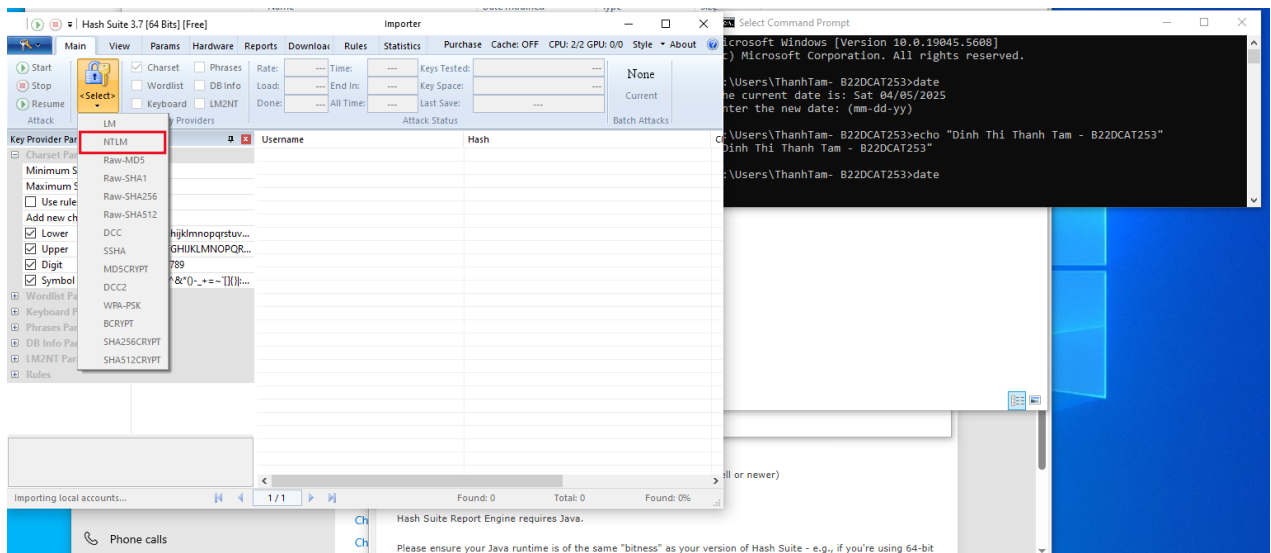


Bước 2: Trích xuất hash người dùng Windows

- Mở HashSuite với quyền Administrator
- Chọn File → Import → From Local Accounts, HashSuite sẽ tự động tải dữ liệu người dùng từ hệ điều hành

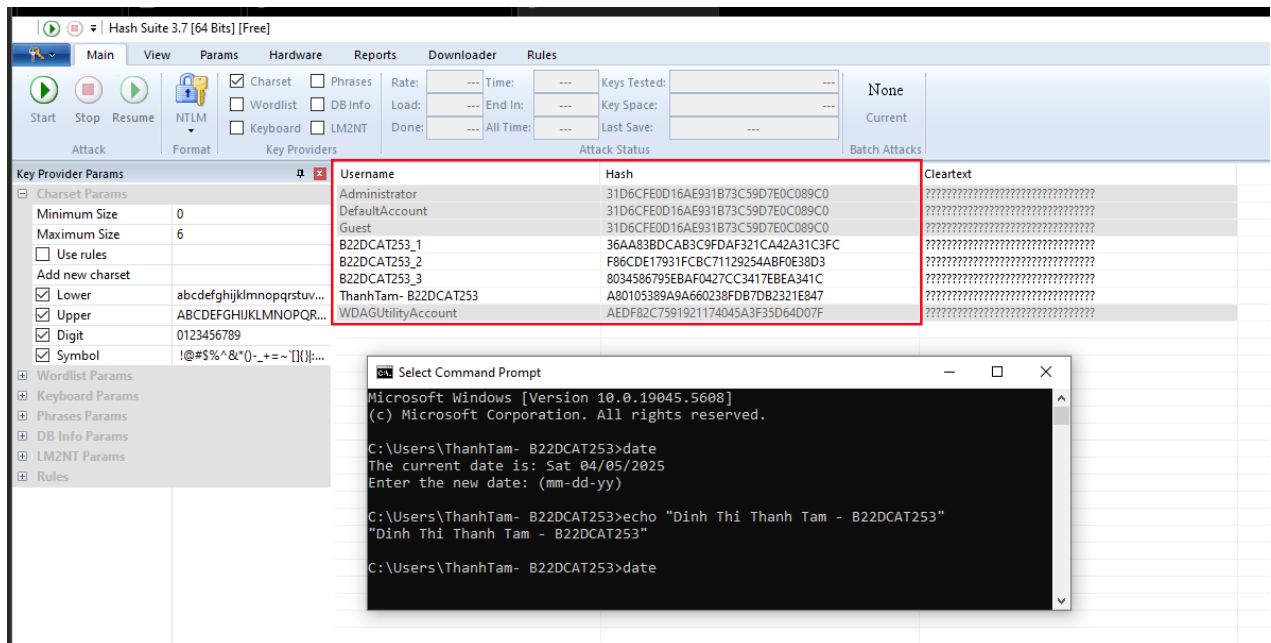


- Ở mục Format chọn NTLM



Bước 3: Tấn công mật khẩu (crack)

- Sau khi import hash thành công, sẽ thấy danh sách user + mã hash tương ứng



- Nhấn Start để bắt đầu Cracking. Chờ đợi một khoảng thời gian để quá trình crack diễn ra

Bước 4: Kết quả

- Sau khi crack thành công, hiển thị mật khẩu gốc của các user

Main View Params Hardware Reports Downloader Rules Statistics

Attack

Format

☐ Charset
☐ Phrases
☒ Wordlist
☐ DB Info
☐ Keyboard
☐ LM2NT

Key Providers

Rate: 441K
Load: 4
Done: 100%

Time: 00:00:00
End In: 00:00:00
All Time: 00:00:00

Keys Tested: 191,488
Key Space: 191,488
Last Save: 00:00:00

Batch Attacks

| Username | Hash | Cleartext |
|----------------------|----------------------------------|----------------------------------|
| Administrator | 31D6CFE0D16AE931B73C59D7E0C089C0 | |
| DefaultAccount | 31D6CFE0D16AE931B73C59D7E0C089C0 | |
| Guest | 31D6CFE0D16AE931B73C59D7E0C089C0 | |
| B22DCAT253_1 | 36AA83BDCAB3C9FDAF321CA42A31C3FC | pass |
| B22DCAT253_2 | F86CDE17931FCBC71129254ABF0E38D3 | pass12 |
| B22DCAT253_3 | 8034586795EBAF0427CC3417EBEA341C | pass1234 |
| ThanhTam- B22DCAT253 | A80105389A9A660238FDB7DB2321E847 | ???????????????????????????????? |
| WDAGUtilityAccount | AEDF82C7591921174045A3F35D64D07F | ???????????????????????????????? |

Command Prompt

```

Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ThanhTam- B22DCAT253>date
The current date is: Sun 04/06/2025
Enter the new date: (mm-dd-yy)

C:\Users\ThanhTam- B22DCAT253>echo "Dinh Thi Thanh Tam - B22DCat253"
"Dinh Thi Thanh Tam - B22DCat253"

C:\Users\ThanhTam- B22DCAT253>

```

KẾT LUẬN

- Crack mật khẩu thành công trên hệ điều hành Windows bằng công cụ Hash Suite
- Crack mật khẩu thành công trên hệ điều hành Linux bằng công cụ John the Ripper

TÀI LIỆU THAM KHẢO

- [1] Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- [2] Chapter 11 Authentication and Remote Access, sách Principles of Computer Security CompTIA Security+ and Beyond Lab Manual (Exam SY0-601) by Jonathan S. Weissman